

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

MINTEL INTERNATIONAL GROUP,)	
LTD., a United Kingdom corporation,)	
)	
Plaintiff/Counter-Defendant,)	Civil Action No. 08-cv-3939
)	
v.)	Hon. Robert M. Dow, Jr.
)	Magistrate Judge Maria Valdez
MEESHAM NEERGHEEN, an individual,)	
)	
)	
Defendant/Counter-Plaintiff)	
_____)	

**NEERGHEEN’S MOTION FOR LEAVE TO FILE, *INSTANTER*,
AN OVERSIZED RESPONSE**

Defendant/ Counter-Plaintiff, Meesham Neergheen, (“Neergheen”), by his attorneys, respectfully moves for leave to file, *instante*, his Opposition to Intel’s Motion for Rule to Show Cause Regarding Temporary Restraining Order and Cross-Motion to Exclude Plaintiff’s Expert’s Affidavit, in excess of fifteen (15) pages. In support thereof, Neergheen states as follows:

1. On August 29, 2008, Plaintiff filed a motion titled “Motion for Rule to Show Cause, For Discovery Sanctions and For Sanctions Because of Evidence Spoliation” (herein, the “Motion). The Motion is fifteen (15) pages in length and is spaced 1.5 lines per inch.
2. Given the length and scope of issues presented in the Motion, and in light of Neergheen’s Cross-Motion relating to the Motion, Defendant respectfully requests that the Court allow him to file, *instante*, his Opposition to Intel’s Motion for Rule to Show Cause Regarding Temporary Restraining Order and Cross-Motion to Exclude Plaintiff’s Expert’s

Affidavit, which is eighteen (18) pages in length, and is double spaced. A copy of Neergheen's Opposition is attached hereto as Exhibit 1.

3. Neergheen believes that Mintel is not prejudiced by allowing the additional pages, as, given spacing differences, the length of the documents is roughly equal.

WHEREFORE, Neergheen respectfully requests that the Court grant this motion and allow him to file, *instanter*, his Opposition to Mintel's Motion for Rule to Show Cause Regarding Temporary Restraining Order and Cross-Motion to Exclude Plaintiff's Expert's Affidavit, in excess of fifteen (15) pages.

Dated: September 4, 2008

/s/ Jeana R. Lervick
John T. Roache
Jeana R. Lervick
Joel C. Griswold
Bell, Boyd & Lloyd LLP
70 West Madison Street
Suite 3100
Chicago, Illinois 60602
312.372.1121
312.827.8000 (facsimile)

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

MINTEL INTERNATIONAL GROUP,)	
LTD., a United Kingdom corporation,)	
)	
)	
Plaintiff/Counter-Defendant,)	Case No. 08-cv-3939
)	Judge Robert Dow, Jr.
v.)	Magistrate Judge Maria Valdez
MEESHAM NEERGHEEN, an individual)	
)	
Defendant/Counter-Plaintiff.)	
_____)	

**OPPOSITION TO MINTEL’S MOTION FOR RULE TO
SHOW CAUSE REGARDING TEMPORARY RESTRAINING
ORDER AND CROSS-MOTION TO EXCLUDE PLAINTIFF’S EXPERT’S AFFIDAVIT**

Defendant/ Counter-Plaintiff Meesham Neergheen (“Neergheen”), by counsel, submits this Opposition to Mintel’s Motion for Rule to Show Cause (“the Motion”) and Cross-Motion to Exclude the Jones Affidavit.

INTRODUCTION

In its Motion to Compel, Mintel makes serious accusations toward Neergheen and these accusations are based entirely upon the affidavit of Mintel’s computer expert, Scott Jones (the “Jones Affidavit”). However, as discussed herein, the Jones Affidavit is, in its entirety, flawed and without basis. The Jones Affidavit makes misstatements, miscalculations, omissions, and leaps in logic that provide no credible support for Mintel’s Motion. What is more, the Jones Affidavit is largely just legal conclusions — a fatal flaw that renders it inadmissible.

Moreover, even if the Jones Affidavit was accurate, at *no* point in time did Neergheen violate either of the Temporary Restraining Order (“TRO”) or any “duty to preserve.” First, the TRO, which in pertinent part is comprised of language *Mintel wrote*, states that Neergheen is not to alter or destroy *Mintel’s documents*. Not even the Jones Affidavit claims Neergheen did so. Second, Mintel drafted the TRO language at the outset of this litigation. In short, to the extent a general duty to preserve exceeds the language of the TRO, Mintel intentionally limited that duty by the terms of the TRO. Third, the general duty to preserve does not, in these circumstances, extend to ceasing all routine use of a computer. In early May 2008, Mintel contacted Neergheen and informed him to simply “not use” the information in the e-mails he sent to himself. Since Mintel was unconcerned about routine use over the course of the next several months, it cannot genuinely claim to be concerned about it now. And fourth, neither the TRO nor the duty to preserve provide for the remedies sought by Mintel. For all of these reasons, Mintel’s Motion is improper and should be denied.

BACKGROUND

On July 11, 2008, Mintel filed an Emergency Motion for Temporary Restraining Order and Injunction. [D.I. 11, 12]. The motion was filed as an emergency despite Mintel knowing for months about the facts it now claims to be at-issue. (*See* Neergheen Opposition to Injunction [D.I. 76]). As part of its Emergency Motion for a TRO, Mintel submitted to the Court a proposed order, setting out precisely the relief it sought. A hearing was held before the Court, and, five days later, the Court entered an Order granting, in part, Mintel's motion. Specifically, the Court granted the precise relief Mintel sought, apart from its request that the Court prevent Neergheen from returning to work. A copy of the Court's Order is attached as Exhibit A.

On July 25, 2008, immediately following the entry of Judge Dow's Agreed Order overseeing the process, Neergheen's expert, Andrew Reisman, provided to Mintel's expert a forensic copy of Neergheen's laptop computer. The copy was provided after extensive discussion by the parties as to the precise protocol for examining the computer. Whether the copy would be produced was not an issue — Neergheen agreed during the hearing for TRO that he would provide the copy. However, in light of privilege and relevancy concerns, the parties sought a proper protocol for review.

As part of the Agreed Order, Mintel agreed that its expert would provide any content found on Neergheen's computer to Neergheen's counsel for review. [D.I. 28]. Neergheen's counsel would then have three (3) days to review the content before producing it to Mintel. *Id.* Following transfer of the forensic copy, Neergheen heard nothing on the topic of when Neergheen's counsel would receive content from Mintel. Despite several requests as to when Neergheen could expect the findings, Mintel's counsel indicated there was nothing yet to provide. Yet on August 13, 2008, during the deposition of Neergheen, Mintel attempted to

question Neergheen about content found by Mintel's expert.¹ Mintel asked, and Neergheen denied, whether Neergheen had taken any of the actions of which it now accuses him. (Ex. B, p. 144). Moreover, during the deposition, counsel implied that Jones had found information other than what he did. In particular, counsel asked:

Q. Isn't it true, sir, that on July 17th you accessed the Microsoft help and support website and entered queries about how to delete data from your computer?

A. Oh, I know exactly. Yes.

Q. Why did you --

A. It wasn't how to delete. I was trying to look for the files that I had sent over to my -- from my Mintel account, and I was trying to find out how to retrieve files from my Hotmail that had been deleted.

(Ex. B, p. 145). At the time the question was asked, counsel for Mintel was aware that, as discussed below, the search Neergheen ran was how to *retrieve* deleted files.

Despite the circumstances, Neergheen's testimony has remained consistent throughout this litigation. Neergheen never opened the e-mails in question, and, following his conversation with Mintel asking that he not do anything with the e-mail contents, he deleted all of them, apart from one that accidentally remained.² Moreover, Neergheen testified that he had, in fact, attempted to *recover* the deleted e-mails that are the subject of Mintel's lawsuit, to demonstrate that he never used their content. (Ex. B, p.148). This testimony is supported by the actual findings on his laptop, as discussed below. Now, as the documents cannot be found on Neergheen's computer, instead of accepting that he is being truthful, Mintel files the present motion, relying solely upon the inaccurate and unreliable Jones Affidavit.

ARGUMENT

Mintel's Motion is entirely based upon the Jones Affidavit and its broad, unsupported and

¹ Mintel's, and Mintel's expert's, violation of the Court's Order is the subject of a currently-pending Motion for Rule to Show Cause.

² Mintel had been on notice of this fact since July 24, 2008, when it received Neergheen's Responses to Mintel's First Set Interrogatories.

generally mistaken conclusions. Mintel cannot demonstrate that any of the allegations wrongly put forth in the Jones Affidavit give rise to spoliation or violation of the TRO. On the face of the TRO, Neergheen did not violate its terms. Further, under the test for spoliation, Neergheen did not violate any inherent duty to preserve.

I. MINTEL BASES ITS MOTION UPON AN, AT BEST, INACCURATE AFFIDAVIT

As its *sole* basis for asserting that Neergheen engaged in pernicious acts, Mintel proffers only a broad, inaccurate, unreliable affidavit from its “expert” Scott Jones. Notably, the Jones Affidavit makes sweeping conclusions that fail to address even the most cursory of forensic reviews. Jones fails immediately by making legal conclusions and jumping to factual suppositions that are easily demonstrated as false. More troubling, when viewed through the eyes of an expert, the Jones Affidavit is wholly inaccurate.

Jones’ affidavit has been examined by Neergheen’s expert, Andrew Reisman (“Reisman”), as set forth in his affidavit attached herein as Exhibit C. More than simply a matter of “competing experts,” Reisman’s findings regarding the Jones Affidavit show the research conducted therein, as well as its conclusions, are patently wrong.

A. The Jones Affidavit is Based on Broad Legal Conclusions and is Therefore Inadmissible

As an initial matter, cursory review of Jones’ affidavit demonstrates its impropriety. Jones extends his opinion beyond the facts and delves into legal argument and supposition. Such is improper, *per se*. *Good Shepard Manor Found., Inc. v. City of Momen*, 323 F.3d 557, 564 (7th Cir. 2003). Expert testimony as to legal conclusions that will affect the outcome of a case is inadmissible. *Id.* (finding “the proffered testimony was largely on purely legal matters and made up solely of legal conclusions,” and thus excluding the expert’s testimony); *see also Perez v. Radioshack Corp.*, 2005 U.S. Dist. LEXIS 36292 at *5-10 (N.D. Ill. Dec. 13, 2005). In the

hearing before Judge Valdez on September 3, 2008, counsel for Mintel made clear that the Jones Affidavit directly affected Mintel's underlying case, not simply the present Motion. [CITE]. Yet Federal Rules of Evidence 702 and 704 prohibit an expert from offering into evidence legal opinions that affect the outcome of a case. FED.R.EVID. 702, 704. Accordingly, on its face, the Jones Affidavit is improper and inadmissible.

In his affidavit, Jones makes broad legal conclusions that are wholly unsupportable. For example, at ¶7 Jones makes the statement (and incorrect assumption, as discussed below) that Neergheen had a duty to preserve that was triggered on July 11, 2008 and that purportedly banned him from turning on his computer. Jones makes further conclusions regarding Neergheen's experience, intent, state of mind, and duties, all of which are improper. This defect was noted by Reisman in his analysis of the Jones Affidavit. After fully examining Jones' allegations Reisman found that the Jones Affidavit:

...reaches erroneous conclusions regarding alleged spoliation of evidence that in some instances are contradicted by the very facts the Affidavit cites, makes sweeping claims about matters beyond the scope of the available data, draws legal conclusions beyond the purview of a forensic examiner, and fails in any fashion to connect the activity cited to loss of any potentially relevant data.
(Ex. C, ¶2).

The mere fact that the Jones Affidavit relies on unsupported legal conclusions warrants it being barred. *See Thomas v. Sheahan*, 514 F. Supp.2d 1083, 1094 (N.D. Ill. 2007)(finding expert's "testimony to the ultimate legal conclusion in this case--that Defendants were 'deliberately indifferent,' or that Cook County had a longstanding practice, custom, or policy of condoning various alleged violations of inmates' rights--is inadmissible.") Similar to *Thomas*, the Jones Affidavit is full of testimony to legal conclusions and is therefore inadmissible.

B. The Jones Affidavit Wrongly Concludes Information is Missing from Neergheen's Computer

The Jones Affidavit at least twice alarmingly concludes that information is missing from Neergheen's computer when, in fact, it is not. Jones improperly and fallaciously states that Neergheen must have deleted Internet history from his computer, and that, in allowing automatic antivirus software to run, Neergheen engaged in intentional destruction of evidence. However, a textbook analysis of Neergheen's computer confirms that no such information was deleted.

At paragraphs 25-28, the Jones Affidavit claims that Neergheen must have deleted Internet history because of "gaps" in daily and weekly entries. However, such entries are not created for every day that a person uses the Internet. (Ex. C, ¶22). By way of example, Reisman demonstrated that fact on his own computer. (*Id.*, ¶¶24-25). While Reisman noted that he has used the Internet regularly, a screenshot of his computer shows a total of eight entries — five from August 2006 and one from July 2007. *Id.* By Jones' logic "these pronounced gaps are the result of a clever attempt to destroy Internet history." (*Id.*, ¶24). Yet Reisman noted he has never taken any steps to delete the files, has used the Internet regularly on the computer, and yet the "gaps" are still present. *Id.* Moreover, Reisman concluded, these perceived "gaps" are not gaps at all. By digging deeper into a forensic analysis of the computer, Jones should have been able to see, as Reisman did, fairly consistent Internet use. (*Id.* ¶26). Accordingly, the "nefariously" missing files on Neergheen's computer are really not missing at all, just as Neergheen has testified.

Similarly, Jones deduces that Neergheen attempted to delete information relating to which USB devices had been inserted into the computer. However, this premise is simply inaccurate. For each of the USB entries listed in the Jones Affidavit at Table Five, there is a corresponding entry with the same date, time and device that is an **active**, non-deleted entry.

(Ex. C, ¶27). Again, the information in question was not deleted at all. Moreover, “ Jones does not explain how the registry data was spoiled given that he could fully view and analyze it.” (*Id.* at ¶30). This is yet another instance of the Jones Affidavit cites to “missing” evidence that is simply not missing. Accordingly, Jones’ serious accusation that Neergheen has taken steps to destroy information on his computer is flawed in light of the fact that the information is not actually missing or destroyed.

C. The Jones Affidavit Wrongly Concludes Neergheen Attempted to Destroy Evidence

Next, the Jones Affidavit claims that allowing antivirus software to run on the computer demonstrates the intentional destruction of evidence. However, not only is allowing an automatic routine function of most computers to run *not* destruction of evidence in violation of a duty to preserve, *the evidence was not destroyed*. The Jones Affidavit states that intentional use of the software obscured date and time metadata. Yet, the evidence Jones claims is missing is readily available from the reports that Jones himself prepared. (Ex. C, ¶17). Jones should have been able to confirm “that the McAfee antivirus software scan does not in fact update last access dates (or upon scanning immediately resets them to their previous state). The only files that would have their last access dates updated are the few files associated with the McAfee program itself....” *Id.* However, Jones failed to do so. Accordingly, Jones’ statement that Neergheen destroyed evidence by allowing the virus scan software to run is simply false.

The Jones Affidavit similarly incorrectly states that over 3,900 file entries were created on or after July 13, 2008 thereby attempting to overwrite files on the computer. Yet, contrary to the Jones Affidavit, Neergheen did not generate anything. Nearly all of the files were related to Internet browsing activity and were thus created by the computer, without aid from Neergheen. *Id.* This is wholly inconsistent with a deliberate attempt to overwrite the hard drive’s unallocated

space. *Id.* Instead, the “newly created” files were a result of simply browsing the Internet. Had Neergheen intended to engage in the acts of which he is accused by Jones, he could have easily done so. He did not. Accordingly, Jones cannot claim that Neergheen’s actions had any more bad faith than simply browsing the Internet as we all do on a daily basis.

Finally, the Jones Affidavit accuses Neergheen of intentionally running a defrag process in an effort to obscure evidence. To the contrary, it is clear that defrag was run on that date as an automated system process rather than the deliberate act of Neergheen, and the very proof of that fact is contained in the Table 7 of the Jones Affidavit. (Ex. C, ¶33). In his affidavit, Reisman discusses at-length how the Jones Affidavit is incorrect. (*Id.*, ¶¶33-43). In his conclusion, Reisman finds that the actions were automatically taken by the computer and would “have had no impact” on the computer for purposes here. Moreover, Reisman found that the actions of which Jones accuses Neergheen would not have resulted in overwriting space as described in Jones’ report. Accordingly, again Jones’ “support” is, at best, inaccurate.

D. The Jones Affidavit Supports Neergheen’s Testimony that He Attempted to Recover the Deleted Files

“The section of the Jones Affidavit entitled ‘Spoliation Noted Within Item 004 Internet History’ establishes what Neergheen already has admitted — that he ran a search in Microsoft’s online support site for ‘how do i access deleted’ files.” (Ex. C, ¶20). During his deposition, Neergheen testified that he had attempted to retrieve the e-mails he deleted when contacted by Mintel in early May 2008. (Ex. B, p. 145). Neergheen so testified even though Mintel counsel misrepresented that the search term found was simply “how to delete.” *Id.* Where Mintel counsel misstated the substance of Neergheen’s search, Jones goes one step further and concludes that, because of the other possible topics Neergheen *could* have searched, he *must* have read one related to how to delete items, and therefore *must* have deleted items (which Jones

himself could not demonstrate). Had Neergheen viewed such help files, it likely would have shown up on the drive. (Ex. C, ¶21). It did not. “Instead, the Jones Affidavit ignores the nature of the search—how to access deleted files, not how to delete files—and cherry picks from the associated hits in the Microsoft Knowledge Base the article that most supports his client’s motion and posits that Mr. Neergheen reviewed that article.” (*Id.*, ¶21). In fact, the computer demonstrates precisely what Neergheen testified to — that he attempted to recover the e-mails he deleted months prior to the present lawsuit. Once again, the Jones Affidavit is amiss.

II. NEERGHEEN DID NOT VIOLATE THE TEMPORARY RESTRAINING ORDER

Mintel’s Motion is based upon the notion that Neergheen violated the TRO entered by the Court. However, given the very clear language of the TRO, this simply cannot be the case. The TRO at issue was *drafted* by Mintel and does not encompass the activities of which Neergheen is now accused.

In relevant part, the TRO states that Neergheen is prohibited from “deleting any files from Defendant’s personal desktop and/or laptop computer **related to or taken from Mintel.**” (Ex. A, p. 14 at E)(emphasis added).³ This language is word-for-word what Mintel proposed to the Court. (Ex. E). The language proposed by Mintel on July 11, 2008 was adopted by the Court on July 16, 2008. Based on its clear language, to which Mintel cannot reasonably now object, Neergheen did not violate the terms of the TRO.

Notably, *nowhere* in the Jones Affidavit is it demonstrated that any of the files, documents, or information presumed by Jones to have been intentionally tampered with have anything to do with the alleged trade secrets at issue. Neergheen testified that he did continue to

³ The remaining provisions of the TRO are unrelated to the present matter. They provide that Neergheen shall not use, reference, evaluate or copy the Mintel documents, shall not reveal or disclose the documents, shall not solicit any client or employee of Mintel, and shall return any Mintel files and provide a copy of his laptop.

use his computer, but only for email and Internet browsing. When asked whether he used his computer, Neergheen stated, “Well, I was checking e-mails, yes, but -- I was using the internet to check e-mails because we -- I was liaisoning with -- I was liaisoning with my attorneys.” (Ex. B, p. 48). When asked explicitly whether any documents were deleted or any other programs were intentionally run, Neergheen answered “No.” *Id.* As discussed above, Neergheen did not destroy evidence and had no intent to do so.

As noted by Mintel in open court, Jones was unable to find any Mintel documents on the laptop — a finding consistent with Neergheen’s testimony that none would be on the computer. The Jones Affidavit fails to demonstrate that any of the allegedly tampered with files, documents or information have anything to do with the alleged trade secrets at issue. The Jones Affidavit does not reference a single file or data artifact that evidence the transmission of Mintel’s purported trade secrets. At no place beyond bald conclusions of wrongdoing does the Jones Affidavit point to any relevant information being intentionally destroyed. As the TRO explicitly sets forth what Neergheen can and cannot do — and as Mintel fails to remotely demonstrate that Neergheen violated its terms — Mintel’s use of a such a flawed argument demonstrates its desperation.

III. NEERGHEEN DID NOT VIOLATE A DUTY TO PRESERVE

The entirety of the Jones Affidavit is based upon the presumption that a party is not entitled to use its computer *at all* following commencement of litigation. Based on this erroneous assumption, Jones concludes that *any* activity on the computer was done with the intent to destroy evidence. Not only is this not legally accurate, it is not a determination to be made by Jones. If Jones’ presumption was correct, then “many companies with regular litigation likely would find [it] challenging meeting that requirement while still performing their normal

business functions.” (Ex. C, ¶7). Reisman inquires whether Mintel held itself to that same standard. *Id.* The deposition of Mintel’s affiant Richard Carr revealed that it did not. (Ex. F, p. 109).⁴

Mintel’s conclusion that Neergheen’s continued use of his laptop is in violation of a duty to preserve evidence is simply inaccurate. While a duty to preserve evidence triggers at the outset of a lawsuit, a party has no duty to preserve information that is not discoverable, and the judgment about what information should be preserved is to be made by the party in possession of the information. *Paul v. USIS Commer. Servs.*, 2007 U.S. Dist. LEXIS 68474 at *3 (D. Col. Sept. 17, 2007). Moreover, to generate an adverse inference as a result of purported failure to preserve, “plaintiffs must demonstrate that defendants (1) had an obligation to preserve the evidence and had control over it when it was destroyed; (2) destruction resulted from defendants’ culpable state of mind; and, (3) the destroyed evidence was relevant to plaintiffs’ case.” *Hamre v. Miza*, 2005 U.S. Dist. LEXIS 8460 at *8 (S.D.N.Y. May 6, 2005). Here, as discussed above, Mintel can show none of these points.

Neergheen testified that he continued to use his computer, but only for email and Internet browsing. (Ex. B, p. 48). When asked explicitly whether any documents were deleted or any other programs were intentionally run, Neergheen answered “No.” *Id.* As discussed above, Neergheen did not destroy evidence. And as he testified he had no intent to do so.

First, Mintel claims that Neergheen’s duty to preserve stems from his receiving notice of the present lawsuit. In doing so, Mintel cites the case *Cohn v. Taco Bell Corp.* as a basis for asserting that “the filing of a complaint alerts a party that certain information is relevant and

⁴ Carr testified that he continued utilizing his work computer after commencement of the present action. He further testified that he had not been asked to produce various e-mails relevant to the present action, which, subsequently, have not been turned over to Neergheen. To-date, counsel for Mintel has failed to respond to Neergheen’s request for the documents.

likely to be sought in discovery.” However, what *Cohn* actually set forth is that “A party clearly is on notice of the relevance of evidence once it receives a discovery request. However, the complaint itself *may* also alert a party that certain information is relevant and likely to be sought in discovery.” *Cohn v. Taco Bell Corp.*, 1995 U.S. Dist. LEXIS 12645 at *14 (N.D. Ill. 1995)(citation omitted)(emphasis added). Of note, Mintel did not provide Neergheen with notice of a duty to preserve — instead, Mintel saw fit to inform *Datamonitor*, a non-party to this matter, of a perceived duty to preserve. Moreover, to the extent Mintel is now appearing to claim that *any* e-mails sent by Neergheen over the course of his ten year career constitute violations (though Mintel has no policy prohibiting such acts), Neergheen could not possibly have been on notice of such a claim at the time of filing. Regardless, the filing of this lawsuit—and Neergheen’s duty according to Mintel—came months after Mintel informed Neergheen that he should simply “not use” the documents it now claims are proprietary. Mintel told Neergheen not to use the documents. Significantly, Mintel did not tell Neergheen to stop using his computer in everyday use. Now, months later, Mintel accuses Neergheen of spoliation for simply using his computer.

Moreover, Mintel intentionally narrowed Neergheen’s duty to preserve by virtue of the TRO it drafted. Filed at the inception of this litigation, Mintel chose to define what Neergheen could and could not do with regard to evidence. It chose to state that he could not destroy Mintel documents—nothing more. And the Court granted Mintel’s request. Accordingly, Mintel cannot claim that a duty beyond what it defined somehow now exists.

Second, as discussed at-length above, Neergheen did not have the requisite state of mind, and no relevant documents or things were destroyed, to give rise to a valid claim of spoliation. As clearly delineated by Reisman, the acts of which Neergheen is accused by the Jones Affidavit

are everyday acts (browsing of the Internet, use of personal e-mail) and involuntary acts (computer's running of antivirus software), neither of which are intentional acts designed to destroy evidence. Moreover, not even the Jones Affidavit can show that evidence was destroyed nor that any such evidence was remotely relevant to the present action.

A. No Relevant Information was “Destroyed”

There are several levels of forensic analysis of a computer. Clearly, the Jones Affidavit demonstrates that Jones engaged in a cursory analysis, at best. However, as set forth by Reisman, further analysis — occasionally even of the “evidence” in Jones’ own affidavit — shows that virtually all of the information Jones claims was destroyed is actually still on the computer.

All of the cases cited by Mintel deal with affirmative destruction of evidence. For example, in *Zubulake v. UBS Warburg, LLC*, the Southern District of New York addressed the intentional destruction of six or more back-up tapes. 2003 U.S. Dist. LEXIS 18771 at *20 (S.D.N.Y. 2003)(finding spoliation but denying adverse inference as a result). Not only is *Zubulake* distinguishable from the present case, it goes on to note that such a preservation does not exist for “identical copies” of documents. *Id.* at *15.

Similarly, in *Siginton v. CB Richard Ellis*, the court found that intentional, willful destruction of evidence occurred. 2003 U.S. Dist. LEXIS 19128 (N.D. Ill. Oct. 24, 2003). However, even under those circumstances, the court still refused to sanction the party that intentionally destroyed documents, as the information was still available on backup tapes. *Id.* *Siginton* is distinguishable, as Neergheen did not intentionally destroy any information. However, even assuming that information from the laptop is “missing” as a result of Neergheen’s use of the computer, Reisman located the same information elsewhere on the hard

drive. Accordingly, the information at-issue is not “missing” for spoliation purposes and sanctions are not warranted.

As discussed above, none of the information Mintel purports to have been destroyed by Neergheen is remotely relevant to the present matter, and the Jones Affidavit does not state otherwise. Even assuming Neergheen’s routine use of the laptop resulted in some inadvertent destruction of certain data, there is no indication that this information is remotely related to the case at bar.

Notably, *none* of the cases relied upon by Mintel regarding relevance support Mintel’s position.⁵ As an initial matter, many of the cases cited for the premise that the information here was relevant were actually decided based on intent of the party and are therefore discussed below. Moreover, *Smith v. United States*, 293 F.3d 984 (7th Cir. 2002), is not only distinguishable, it supports Neergheen’s position. *Smith* involved the dismissal of a veteran’s claims to title to an Army tank, and his destruction of the tank in question. The Seventh Circuit stated “[s]poliation of evidence does not apply in this case because the [evidence that was destroyed] shed no light on Smith’s claims.” *Id.* at 988. Similarly in *Diersen v. Walker* (2003 U.S. Dist. LEXIS 9538 (N.D. Ill. June 5, 2003), the court denied a motion for sanctions based on alleged spoliation. The *Diersen* court found sanctions were not warranted because “[a]lthough GAO failed to preserve certain limited documents, the facts surrounding their destruction do not support an inference that the destroyed documents would have been unfavorable to GAO.” *Id.* Mintel cannot demonstrate that any documents or information relevant to the present case were destroyed by Neergheen, and cannot cite to any case law supporting its position.

⁵ *China Ocean Shipping Co. v. Simone Metals* is wholly unrelated to the questions at-issue. 1999 U.S. Dist. LEXIS 16229 (N.D. Ill. Oct. 1 1999). The court in *China Ocean* denied a motion for summary judgment on spoliation, finding spoliation to be a question of fact. Whether spoliation occurred was not at-issue.

B. Neergheen Did Not Intend to Destroy Evidence

Further, Mintel's broad accusations of wrongdoing cannot demonstrate any intent on the part of Neergheen to destroy documents. Neergheen testified that he used the computer, but did so only to browse the Internet, attempt to *recover* documents deleted months earlier that he thought relevant, and correspond with his attorneys. (Ex. B, p. 48). Mintel claims that Neergheen "lied, under oath" regarding laptop usage, and cites Neergheen's testimony in which he states he did not stop using his computer." (Motion p. 12). This is nothing short of a misrepresentation to the Court. As noted above, Neergheen's actual testimony reflected that he did use the computer, for routine uses. (Ex. B, p. 48). Nothing indicates Neergheen acted intentionally so as to destroy evidence. Moreover, Mintel's argument to the contrary is circular — it argues that he is not trustworthy because he destroyed evidence and that its only proof he destroyed evidence is that he is untrustworthy. This logic is as flawed as the Jones Affidavit.

Of note, several of the cases cited by Mintel's Motion regarding intent are also actually contrary to Mintel's position. In *Crabree v. Natl. Steel Corp.*, the Seventh Circuit affirmed the district court's exclusion of evidence of destruction of documents. 261 F.3d 715 (7th Cir. 2001). The court found that there was no bad faith in the documents' destruction and, accordingly, such evidence was properly excluded. *Id.* Similarly, in *Boyd v. Travelers Ins. Co.*, the Supreme Court of Illinois addressed a party's taking from the defendant the physical item at the heart of the issue, then "losing" it. 166 Ill.2d 188 (Ill. 1995). Yet, even under such circumstances, the Court *still* found that the moving party could not show the destruction was intentional. *Id.* at 203.

The remaining cases are clearly distinguishable. Mintel cites *RKI, Inc. v. Grimes*, 177 F. Supp.2d 859 (N.D. Ill. 2001) in support of its proposition that mere defragmentation of a computer gives rise to an inference of wrongdoing. (Motion p. 8). However, this is not what

Grimes states.⁶ The *Grimes* court found that the defendant employee had engaged in several underhanded activities including: (1) intentionally defragmenting his computer four times over the span of a few days without explanation; (2) lying about why he did so by claiming a third-party computer store told him to defragment the computer; and, (3) undertaking these acts to hide use of his former employer's trade secrets to solicit business in his new employment. *Grimes*, 177 F. Supp.2d at 870. Indeed, the defendant in that case told co-workers that he had used customer information to steal customers from his former employer and "was looking forward to stealing all of [his former employer's] customers and that he had a lot of customers that were coming with him." *Id.* at 868. In this case, there is no evidence of any such acts. As Reisman explains, defragmentation of Neergheen's computer was a result of an involuntary process. Far from the actions of the defendant in *Grimes*, here Neergheen did not intentionally run the program and certainly did not do so multiple times in a concerted effort to hide evidence. The fact that the program ran does not relate in any way to a intent on the part of Neergheen.

Similarly, Mintel's reliance upon *Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.* is severely misguided. In fact, Mintel misrepresents to the holding in *Kucala*. In *Kucala*, the court found spoliation where a party had actually purchased, installed, and used a computer program called the "Evidence Eliminator," designed for the purpose of deleting files. 2003 U.S. Dist. LEXIS 8833 (N.D. Ill. 2003). Notably, contrary to Mintel's assertions in its brief, the party in *Kucala* did not "defrag the drive." *Id.* Instead, it was the active purchase of software designed for the purpose of destroying evidence that led the court in *Kucala* to find spoliation.

IV. MINTEL IS NOT ENTITLED TO THE RELIEF IT SEEKS

Finally, the relief sought by Mintel far overreaches that to which it would have been

⁶ The *Grimes* court also noted that defragmentation is "called for when computer files and data are more than 10% fragmented." *Id.* The court recognized the legitimate purposes of defragmentation, only chose to infer negative purpose *in that case* due to other circumstances.

entitled had it been able to demonstrate spoliation.

Mintel cannot demonstrate the acts alleged in the Jones Affidavit caused it damage. Again, at no point is it demonstrated that any information relevant to the present matter was destroyed through routine use of Neergheen's computer. The only case cited by Mintel for the proposition it has been harmed is *Metropolitan Opera Ass'n, Inc. v. Local 100*. 2003 U.S. Dist. LEXIS 1077 (S.D.N.Y. Jan 28, 2003). However, in *Metropolitan Opera*, the New York district court addressed a consistent failure on the part of a party to investigate the factual basis for its discovery responses. The court addressed a series of affirmative steps by the responding party that violated the Federal Rules, the cumulative effect of which was prejudice. Such is not the case here. Moreover, in another case cited by Mintel, *Boyd v. Travelers Ins. Co.*, the Supreme Court of Illinois found that, in order to demonstrate spoliation, a plaintiff must **prove** he suffered **compensable** damages as a result of the destruction. 166 Ill.2d 196. Mintel cannot do so here.

It is well-settled law that sanctions in the form sought by Mintel are extreme and rarely justified. Spoliation of evidence sometimes permits, but rarely **if ever** requires the peremptory remedy of dismissal of a case. See *Mathis v. John Morden Buick, Inc.*, 136 F.3d 1153 (7th Cir. 1998).⁷ "Because a default judgment deprives a party of a hearing on the merits, the harsh nature of this sanction should usually be employed in extreme situations where there is evidence of willfulness, bad faith, or fault by the noncomplying party." *Diersen*, 2003 U.S. Dist. LEXIS at *10. "Bad faith" has been held to mean destruction "for the purpose of hiding adverse information." *Id.*, quoting, *Mathis v. John Morden Buick, Inc.*, 136 F.3d 1153, 1155 (7th Cir. 1998). The sanction sought by Mintel "is especially inappropriate where the proof of willful and bad faith destruction is wanting or it is clear that a party's ability to prosecute the case has not

⁷ The cases cited by Mintel in support of its position default judgment/ dismissal is proper are addressed above and are demonstrated as distinguishable and/ or supportive of Neergheen's position.

been meaningfully compromised.” *Rodgers v. Lowe’s Home Centers, Inc.*, 2007 U.S. Dist. LEXIS 7405 at *2 (N.D. Ill. Jan. 30, 2007), *citing*, *Maynard v. Nygren*, 332 F.3d 462, 467 (7th Cir. 2003). Here, Mintel cannot show bad faith, that any relevant information has been destroyed, nor that its case has been compromised. Accordingly, a default judgment is wholly inappropriate.

In this regard, Mintel’s request for money, too, is inappropriate. Mintel bases its request on 37(a)(4)(A) and the case *Illinois Tool Works, Inc. v. Metro mark Products, Ltd.*, 43 F. Supp.2d 951, 960 (N.D. Ill. 1999). However, both 37(a)(4)(A) and *Illinois Tool Works* deal with violations in connection with a motion to compel. *Id.*; Fed.R.Civ.P. 37(a)(4)(A). Again, such is not the case here. Moreover, to the extent such sanctions are allowable, they clearly are not warranted as discussed above.

CONCLUSION

As set forth above, Mintel’s Motion is without merit and should be denied in its entirety. Moreover, in light of the legal conclusions reached in the Jones Affidavit, Neergheen respectfully submits that the document should be excluded from these proceedings as improper.

Dated: September 4, 2008

 /s/ Jeana R. Lervick
 John T. Roache
 Jeana R. Lervick
 Joel C. Griswold
 Bell, Boyd & Lloyd LLP
 70 West Madison Street
 Suite 3100
 Chicago, Illinois 60602
 312.372.1121
 312.827.8000 (facsimile)

EXHIBIT A

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

MINTEL INTERNATIONAL GROUP,
LTD., a United Kingdom corporation,

Plaintiff,

v.

MEESHAM NEERGHEEN, an individual,

Defendant.

)
)
)
)
)
)
)
)
)
)
)

CASE NO.: 08-CV-3939

MEMORANDUM OPINION AND ORDER

On July 11, 2008, Plaintiff Intel International Group, Ltd. (“Intel”), filed a seven-count complaint against Defendant Meesham Neergheen (“Neergheen”) alleging a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.*, a violation of a non-compete agreement, a breach of Neergheen’s employment contract with Intel, and misappropriation of trade secrets pursuant to the Illinois Trade Secret Act (“ITSA”), 765 ILCS 1065/1, *et seq.* Plaintiff seeks injunctive relief, restitution, and compensatory and punitive damages. Also on July 11, 2008, Plaintiff filed an emergency motion for a temporary restraining order and preliminary injunction.

On July 15, 2008, the Court conducted a hearing on Plaintiff’s request for a temporary restraining order (“TRO”). At the hearing, Defendant Neergheen was represented by counsel who, despite not having sufficient time to file a written response to the motion for a TRO, articulated Defendant’s position with respect to the relief requested by Plaintiff. Having considered the relevant legal standards governing TROs, as well as Plaintiff’s motion, memorandum, and supporting materials and defense counsel’s comments at the hearing, the Court grants in part and denies in part Plaintiff’s emergency motion.

I. Background

Mintel is headquartered in London, England and provides consumer, product, and market research to its clients around the world. Cmplt., ¶¶ 2, 6. Neergheen worked for Mintel's marketing department from June 30, 1997 until April 30, 2008. During that time, Neergheen had access to client and marketing files and materials. On or about June 24, 1998, Neergheen signed a Contract of Employment with Mintel. Carr Affdt., ¶ 8. The Contract of Employment contained a clause stating that Neergheen could not directly or indirectly compete with Mintel for the first twelve months after the end of Neergheen's employment with Mintel. *Id.* The Contract of Employment also stated that Neergheen must refrain from using or disclosing any of Mintel's trade secrets and other proprietary or confidential information. *Id.*

In August 2003, Neergheen signed an Employee Non-Compete/Non-Solicitation Agreement ("Non-Compete Agreement"). Carr Affdt., ¶ 9. The Non-Compete Agreement stated that Neergheen agreed not to compete with the business of Mintel or any of its subsidiaries for a period of one year. *Id.* The Non-Compete Agreement also included a confidentiality provision that stated that Neergheen was not to disclose any information of a confidential or proprietary nature. *Id.*

Mintel avers that it has a secure computer network and secure server system that is configured and managed to prevent unauthorized access. Thomson Affdt., ¶ 3. Mintel also states that as a result of Neergheen's employment and position with Mintel, he had access to such confidential information and became familiar with Mintel's computer system. *Id.*, ¶ 5.

On or about April 23, 2008, Neergheen provided written notice to Mintel that he would be resigning from Mintel effective April 30, 2008. Carr Affdt., ¶ 10. After receiving Neergheen's written notification, Mintel began searching and monitoring Neergheen's work computer. Thomson Affdt., ¶ 6. Mintel subsequently discovered that Neergheen had copied, e-mailed and/or printed certain confidential and proprietary files – including client lists, vendor lists, and strategic

documents – from his work computer on April 29, 2008, the day before his departure from Mintel. Thomson Affdt., ¶ 7.

In its complaint, Mintel alleged that Neergheen commenced employment with Datamonitor, Inc., a competitor of Mintel, immediately after Neergheen's resignation from Mintel. Cmpl't., ¶ 17; Carr Affdt., ¶ 14. Based on additional information provided during and after the hearing on July 15, 2008, it appears that Neergheen started his new job at the end of May and that he was told not to come to work on July 14 or 15 or until the Court issues an order on the TRO.

II. Discussion

A party seeking a temporary restraining order must demonstrate as a threshold matter that (1) its case has some likelihood of succeeding on the merits; (2) no adequate remedy at law exists; and (3) it will suffer irreparable harm if preliminary relief is denied. *Abbott Laboratories v. Mead Johnson & Co.*, 971 F.2d 6, 11 (7th Cir. 1992). If the moving party meets this burden, the court weighs these factors along with any irreparable harm the non-moving party will suffer if preliminary relief is granted, balancing that harm against the irreparable harm to the moving party if relief is denied. *Id.* Finally, the court considers the public interest served by granting or denying the injunction, including the effects of the injunction on non-parties. *Id.*; see also *Credit Suisse First Boston, LLC v. Vender*, 2004 WL 2806191, at *1 (N.D. Ill. December 3, 2004).

A. Likelihood of Success

The party seeking the TRO or preliminary injunction must demonstrate “some likelihood of succeeding on the merits.” *Abbott Laboratories*, 971 F.2d at 11; see also *Frullati Franchise Sys., Inc. v. Dana Areece & Co., Inc.*, 2001 WL 743427, at *2 (N.D. Ill. June 28, 2001) (stating that for purposes of a TRO or preliminary injunction, a plaintiff need only establish a “trivial chance of succeeding on the merits”) (citing *Green River Bottling Co. v. Green River Corp.*, 997 F.2d 359, 361 (7th Cir. 1993)).

I. Violation of the Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, provides for the entry of civil injunctive relief as well as the recovery of money damages for a violation of its provisions. See 18 U.S.C. § 1030(g) (providing that “[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief”). Courts have upheld the use of the CFAA in granting injunctive relief against former employees and their new employers who have attempted to obtain a competitive edge by removing information from a former employer’s computers. See, e.g., *YourNetDating, LLC v. Mitchell*, 88 F. Supp. 2d 870, 872 (N.D. Ill. 2000) (granting TRO under CFAA claim against former employee); see also *Charles Schwab & Co., Inc. v. Carter*, 2005 WL 351929, at *3 (N.D. Ill. Feb. 11, 2005) (denying motion to dismiss claim under CFAA); *George S. May Int’l Co. v. Hostetler*, 2004 WL 1197395, at *3 (N.D. Ill. May 28, 2004).

The day before Neergheen’s resignation, Neergheen copied, e-mailed to his personal e-mail address and/or printed information from his work computer. See Thomson Affdt., ¶ 7. According to Mintel’s supporting affidavits, those files contained confidential and proprietary information regarding client accounts and budgets, potential client lists, vendor lists, marketing strategies and overall objectives, and individual client cost data. Carr Affdt., ¶ 13. Neergheen’s actions in e-mailing such information to his personal e-mail address in the days leading up to his resignation could be found to have “exceeded authorized access” as that term is defined in 18 U.S.C. § 1030(e)(6). Because Mintel’s allegations, if proven, appear to be sufficient to give rise to liability for a violation of the CFAA, the Court finds that Plaintiff has demonstrated some likelihood of success on the merits of its CFAA claim. See *YourNetDating, LLC*, 88 F. Supp. 2d at 872.

2. *Violation of the Illinois Trade Secret Act*

The Illinois Trade Secret Act, 765 ILCS 1065/1, *et seq.*, defines a “trade secret” as information that:

- (i) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and
- (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.

See 765 ILCS 1065/2(d). The ITSA defines “misappropriation” in several ways. For example, one can misappropriate trade secrets by “acquiring” them through improper means such as the breach of a confidential relationship. 765 ILCS 1065(b)(1).¹ Misappropriation also occurs when a defendant breaches a duty owed to protect the secrecy of its information or induces another party to do so. 765 ILCS 1065(b)(2)(B).

Mintel alleges that the various files copied, e-mailed and/or printed by Neergheen in the days leading up to his resignation contained highly sensitive information not disseminated into the public domain. Carr Affdt., ¶ 13. As with its CFAA claim, if Mintel is able to prove its allegations, then Neergheen may well have violated the ITSA. At this stage, that is sufficient to meet the threshold requirement of showing some likelihood of success on the merits.

3. *Violation of restrictive covenants within Non-Compete Agreement and Contract of Employment*

Based on the Court’s preliminary research, it appears that Illinois courts disfavor and closely scrutinize restrictive covenants because they are “repugnant to the public policy encouraging an open and competitive marketplace.” *Roberge v. Qualiteck Int’l, Inc.*, 2002 WL

¹ As defined in the Act, “improper means” includes theft, bribery, misrepresentation, breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use, or espionage through electronic or other means. 765 ILCS 1065(a).

109360, at *4 (N.D. Ill. Jan. 28, 2002) (citing *Bishop v. Lakeland Animal Hosp.*, 268 Ill.App.3d 114, 644 N.E.2d 33, 36 (Ill. App. Ct. 1994)). The basic test applied by Illinois courts in determining the enforceability of a restrictive covenant is “whether the terms of the agreement are reasonable and necessary to protect a legitimate business interest of the employer.” *Outsource Intern., Inc. v. Barton*, 192 F.3d 662, 666 (7th Cir. 1999) (quoting *Office Mates 5, North Shore, Inc. v. Hazen*, 234 Ill. App. 3d 557, 599 N.E.2d 1072, 1080 (1992)). This determination “necessarily turns on the facts and circumstances of each case.” *Id.* Illinois law requires that in order be enforceable, a covenant not to compete must secure a “protectable interest” of the employer. *Curtis 1000, Inc. v. Suess*, 24 F.3d 941, 944 (7th Cir. 1994). Illinois courts recognize at least two such protectable interests: (1) where the customer relationships are near-permanent and but for the employee’s association with the employer the employee would not have had contact with the customers; and (2) where the former employee acquired trade secrets or other confidential information through his employment and subsequently tried to use it for his own benefit. *Outsource Int’l, Inc. v. Barton*, 192 F.3d 662, 666 (7th Cir. 1999).

Restrictive covenants should be narrowly tailored so as only to protect the protectable interest of the employer. *Id.* at 669; *Lawrence and Allen, Inc. v. Cambridge Human Resource Group, Inc.*, 292 Ill.App.3d 131, 138, 685 N.E.2d 434, 441 (Ill. App. Ct. 1997). In particular, the time and geographic limitations must be reasonably necessary to protect a legitimate business interest of the employer. *Roberge*, 2002 WL 109360, at *4. A restrictive covenant that does not contain a geographic limitation may still be enforceable if the covenant instead includes an “activity restraint.” *Id.* at *6. The most common type of activity restraint is a prohibition against soliciting the former employer’s customers. *Eichman v. Nat’l Hosp. and Health Care Servs., Inc.*, 308 Ill.App.3d 337, 719 N.E.2d 1141, 1147 (Ill. App. Ct. 1999).

Neergheen commenced employment with Mintel in its London office on or about June 30, 1997. Carr Affdt., ¶ 6. As a condition of his continued employment, Neergheen signed and executed a United Kingdom Contract of Employment with Mintel on or about June 24, 1998. Carr Affdt., ¶ 8. The Contract of Employment included the following restrictive covenant:

You will not for the first twelve months at the end of your employment with us, either on your own account or on behalf of any other legal person and in competition with the Company, or any subsidiary directly or indirectly engage in, or be connected with, trade or business carried on by us or any of our associates at the end of your employment. ... You will not, for the first twelve months after the end of your employment with us, solicit away from us or our associates any person who is and was, when your employment ended, employed by us or an associate as a director, senior manager or sales person for whom you were responsible, or who was a member of any department/project/team in which you worked during the last twelve months of your employment.

Cmplt., ¶ 13.

On or about August 1, 2003, Neergheen transferred to Mintel's Chicago office. Carr Affdt., ¶ 6. As a condition of his continued employment with Mintel in Chicago, Neergheen agreed to and signed an Employee Non-Compete/Non-Solicitation Agreement ("Non-Compete Agreement") on August 4, 2003. Carr Affdt., ¶ 9. The Non-Compete Agreement signed by Neergheen stated as follows:

The undersigned Employee hereby agrees not to compete, either directly or indirectly, with the business of Mintel or any of its subsidiaries, branches or divisions, at any location worldwide at any time during the Employee's term of employment, and for a period of one (1) year following his termination of employment with Mintel, regardless of the reason or cause for such termination.

Cmplt., ¶ 10.

At this stage, based on the record before the Court, it appears that Mintel has a strong likelihood of success on its claim that Neergheen violated at least some of the terms of his non-compete agreement and employment contract. However, in order for the Court to uphold the provisions at issue, those provisions must be enforceable under Illinois law. Although Mintel

asserts that these restrictive covenants are both reasonable as to time and geography, the Court does not have before it at this early stage of the case either the factual record or the legal support grounded in Illinois cases to be convinced that every provision that Mintel seeks to enforce ultimately can be sustained as a matter of law. Among other things, the Court lacks sufficient information concerning (1) the circumstances of Defendant's departure from Mintel; (2) the circumstances of Defendant's hiring by Datamonitor; and (3) Defendant's new position and responsibilities at Datamonitor.

Despite the limited record, the Court concludes that Mintel has "some" likelihood of successfully demonstrating that some, if not all, provisions of its restrictive covenants are reasonable under the law of Illinois. The Court further finds that Plaintiff has satisfied its burden of demonstrating "some likelihood of succeeding on the merits" of its claim that Neergheen violated at least some, if not all, of the restrictive covenants in the non-compete agreement and his employment contract.

B. Adequate Remedy at Law and Irreparable Harm

The other two threshold elements that Mintel must prove to support the issuance of a TRO or a preliminary injunction are that it (1) has no adequate remedy at law and (2) will suffer irreparable harm if the injunction is not issued. These two requirements – irreparable harm and no adequate remedy at law – tend to merge. See *Roland Machinery Co. v. Dresser Indus., Inc.*, 749 F.2d 380, 387 (7th Cir. 1984). "The question is then whether the plaintiff will be made whole if he prevails on the merits and is awarded damages." *Id.* An injury is "irreparable" when it is of such a nature that the injured party cannot be adequately compensated in damages or when damages cannot be measured by any pecuniary standard. *Meridian Mut. Ins. Co. v. Meridian Ins. Group, Inc.*, 128 F.3d 1111, 1120 (7th Cir. 1997); see also *Gateway Eastern Ry. Co. v. Terminal R.R. Ass'n of St. Louis*, 35 F.3d 1134, 1140 (7th Cir. 1994) ("showing injury to

goodwill can constitute irreparable harm that is not compensable by an award of money damages”).

Here, Mintel contends that it will be unable to repair the damage done to its business relations with its existing customers and will lose the competitive advantage that it has worked to establish. Carr Affdt., ¶ 16. The loss of clients and sales and the continuing threat of further loss due to the distribution of Mintel’s client lists and marketing data are sufficient to constitute irreparable injury. See *Meridian Mut. Ins. Co.*, 128 F.3d at 1120; see also *Illinois Sporting Goods Assoc. v. County of Cook*, 845 F. Supp. 582, 585 (N.D. Ill. 1994) (finding irreparable harm because of threat to the existence of plaintiff’s business).

Moreover, money damages likely would not be an adequate remedy in the present case. First, Mintel could face the threat of lost sales and clients if Neergheen does use the information he removed from Mintel’s computer system prior to leaving his employment. Second, it is difficult, at this time, to ascertain with any certainty the degree of financial loss Mintel may suffer by virtue of Neergheen’s conduct. It is well recognized that in circumstances like the present, irreparable harm includes the impossibility of ascertaining with any accuracy the extent of the loss. It is also difficult to determine at this time the extent to which Mintel’s confidential information could (or would) be utilized by Neergheen and Datamonitor. Given these circumstances, the Court finds that Plaintiff has demonstrated that money damages would be an inadequate remedy, at least for the duration of the TRO.

C. Balancing the Harms and Public Interest

Balancing the irreparable harm to the moving party if an injunction is not entered against the harm to the non-moving party if an injunction is granted requires the court to use a “sliding-scale approach; the more likely the plaintiff will succeed on the merits, the less the balance of irreparable harms need favor the plaintiff’s position.” *In re Aimster Copyright Litigation*, 252 F.

Supp. 2d 634, 648 (N.D. Ill. 2002). Most of the injunctive relief sought by Mintel relates to the confidential information that Neergheen is alleged to have removed from Mintel's computers. Granting the requested relief to that extent only would prohibit Neergheen from using material that it appears he should not have taken in the first place. Therefore, any harm that he may suffer for the brief duration of the TRO would be in large part a consequence of his own conduct in the days leading up to his departure from Mintel.

The other injunctive relief that Mintel seeks pertains to the non-solicitation and non-compete provisions of Neergheen's employment agreements. As to the former, the Court finds that the balance of the harms weighs in favor of granting the requested relief. However, at this stage of the case and based on the current record, the Court cannot conclude that the balance of harms militates in favor of entering temporary injunctive relief on the non-compete provisions. Nor can the Court say with any degree of confidence that Mintel has a likelihood of success with respect to those provisions. In reaching that conclusion, the Court is guided by the settled propositions that a TRO is an extraordinary remedy and that it is Plaintiff's burden to show a clear entitlement to relief. Given those propositions, the Court cannot conclude that Defendant should be enjoined from working in his new position, at least during the short time period between the entry of the TRO and the hearing date on the motion for preliminary injunction. See *Credit Suisse First Boston, LLC v. Vender*, 2004 WL 2806191, at *4 (N.D. Ill. December 3, 2004). That conclusion in no way prejudices the Court's ultimate ruling on the enforceability of the non-compete provisions once the Court has a more complete factual record and the benefit of additional briefing from both parties.

D. Public Interest

Finally, the Court concludes that the public interest cuts both ways in this case. On the one hand, the public has a significant interest in enforcing contracts and preventing violations of

statutes. Yet, as noted above, there is a countervailing interest in an open and competitive marketplace and in enforcing only reasonable terms of non-compete agreements. At this stage of the case, the Court views these competing public interest considerations to be in equipoise.

III. Conclusion

Based on the foregoing, the Court grants in part and denies in part Plaintiff's emergency motion for a temporary restraining order and preliminary injunction and orders as follows:

1. Based upon the pleadings and affidavits filed by Plaintiff and the arguments of counsel in open court, the Court finds that Plaintiff has sustained its burden and demonstrated some likelihood of success on the merits of its claims. The Court also finds that Plaintiff likely does not possess an adequate remedy at law and will suffer irreparable harm should a temporary restraining order not be issued. Finally, the balance of harms and public interest also are served by the issuance of a temporary restraining order as to certain of Plaintiff's requests as identified above.

2. Pursuant to Federal Rule of Civil Procedure 65(b), a ten (10) day temporary restraining order, commencing at 2:30 p.m. on July 16, 2008 and expiring at 2:30 p.m. on July 30, 2008, is entered upon the following terms and conditions:

- A. Defendant, his agents, servants, employees, officers, attorneys, successors and assigns, and all persons, firms, and corporations acting in connection or participation with him or on his behalf, are enjoined from using, referencing, evaluating, or copying all originals and copies of information or documents misappropriated from Mintel in hard copy or electronically stored;
- B. Defendant, his agents, servants, employees, officers, attorneys, successors and assigns, and all persons, firms, and corporations acting in connection or participation with him or on his behalf, are enjoined from revealing or disclosing in any manner information and documents misappropriated from Mintel in hard copy or electronically stored;

- C. Defendant is required to return to Mintel all copied, printed, and/or downloaded files, materials, and information taken from Mintel;²
- D. Defendant is required to produce forensic copies of all personal desktop and/or laptop computers;
- E. Defendant, his agents, servants, employees, officers, attorneys, successors and assigns, and all persons, firms, and corporations acting in connection or participation with him or on his behalf, are prohibited from deleting any files from Defendant's personal desktop and/or laptop computer related to or taken from Mintel;
- F. Defendant is prohibited from contacting or soliciting any Mintel customer or client that Defendant had contact with during the last twelve (12) months of his respective employments with Mintel;
- G. Defendant is prohibited from soliciting or contacting any Mintel employee for purposes of working at Datamonitor or any other competitor of Mintel.

3. Plaintiff's request for expedited discovery is granted. The parties may commence discovery at once. Written discovery responses are due within seven (7) days of service. Defendant shall appear for his deposition within ten (10) days.

4. This matter is set for a preliminary injunction hearing on Monday, August 4, 2008 at 10:30 a.m. in Room 1919. Further details on briefing and other scheduling matters are addressed in a separate minute order.



Dated: July 16, 2008

Robert M. Dow, Jr.
United States District Judge

² As discussed at the July 15 hearing, counsel for Defendant may keep a copy of these materials for purposes of this litigation only.

EXHIBIT B

Neergheen, Meesham 8/13/2008 9:44:00 AM

1 IN THE DISTRICT COURT OF THE UNITED STATES
2 FOR THE NORTHERN DISTRICT OF ILLINOIS
3 EASTERN DIVISION
4

MINTEL INTERNATIONAL GROUP,)
5 LTD., a United Kingdom)
corporation,)
6)
Plaintiff,)
7)
-vs -) No. 08 CV 3939

8)
MEESHAM NEERGHEEN, an)
9 individual)
)
10 Defendant.)
11

12 The videotaped deposition of
13 MEESHAM NEERGHEEN, called for examination
14 pursuant to notice and the Rules of Civil
15 Procedure for the United States District Courts
16 pertaining to the taking of depositions, taken
17 before Allison D. Weber, CSR, a notary public
18 within and for the County of Cook and State of
19 Illinois, at 33 West Monroe Street, Suite 2700,
20 Chicago, Illinois, on the 13th day of August,
21 2008, at the hour of 9:44 o'clock a.m.
22
23

Reported by: Allison D. Weber, CSR
24 License No.: 084-002238

Neergheen, Meesham 8/13/2008 9:44:00 AM

1 A. Did I do anything?

2 Q. Did you stop using it?

3 A. My laptop?

4 Q. Yes.

5 A. I think I may have printed out the
6 documents just so that I could have a copy,
7 because when I brought the copy that was
8 delivered by messenger into the office, I left it
9 with Richard Watkins.

10 Q. Did you keep using your computer?

11 A. No. No.

12 Q. You stopped using it entirely after --

13 A. Well, I was checking e-mails, yes,
14 but -- I was using the internet to check e-mails
15 because we -- I was liaisoning with -- I was
16 liaisoning with my attorneys.

17 Q. Did you delete any documents from
18 your computer from the time you received the
19 complaint until the time you turned it over to
20 counsel?

21 A. No.

22 Q. Aside from accessing the internet --
23 using the internet to access your e-mail, did you
24 do anything else with the computer, run any other

Neergheen, Meesham 8/13/2008 9:44:00 AM

1 Q. Do you know what a defrag program

2 is?

3 A. No.

4 Q. Are you aware that a defrag program was

5 run on your computer on July 14th?

6 A. I don't know.

7 Q. Do you have any explanation as to why it

8 would have been run on your computer on

9 July 14th?

10 A. I don't know.

11 Q. Would it surprise you if a defrag

12 program had been run on your computer on

13 July 14th?

14 A. I don't know what a defrag program is.

15 Q. You're aware that an antivirus program

16 ran on your computer on July 17th?

17 A. I don't know.

18 Q. You're aware that that would write over

19 files?

20 A. I don't know.

21 Q. Are you aware of your duty to preserve

22 evidence in this case?

23 A. I'm sorry?

24 Q. Are you aware of your duty to preserve

Neergheen, Meesham 8/13/2008 9:44:00 AM

1 evidence in this case?

2 A. Can you explain that?

3 Q. You're aware that once you had notice of
4 this lawsuit you weren't supposed to be using
5 your computer?

6 MR. ROACHE: Object to the form.

7 THE WITNESS: Um, I don't know.

8 BY MR. PIOLI:

9 Q. Nobody ever informed you about a
10 duty to preserve evidence in this case?

11 A. I don't know.

12 Q. Isn't it true, sir, that on July 17th
13 you accessed the Microsoft help and support
14 website and entered queries about how to delete
15 data from your computer?

16 A. Oh, I know exactly. Yes.

17 Q. Why did you --

18 A. It wasn't how to delete. I was trying
19 to look for the files that I had sent over to
20 my -- from my Mintel account, and I was trying to
21 find out how to retrieve files from my Hotmail
22 that had been deleted.

23 Q. What searches did you enter?

24 A. I can't remember.

Neergheen, Meesham 8/13/2008 9:44:00 AM

1 instructed you not to answer those questions.

2 Are you going to heed your counsel's

3 advice and not answer those questions?

4 MR. ROACHE: I believe he did. We can go

5 back and look, but I think he answered them even

6 though I instructed him not to.

7 MR. PIOLI: Are you claiming privilege with

8 regard to those answers?

9 MR. ROACHE: I'm not.

10 MR. PIOLI: You're not?

11 MR. ROACHE: No.

12 MR. PIOLI: I'd like those questions

13 certified, the two questions that he refused to

14 answer on the advice of counsel.

15 MR. ROACHE: Which two did he refuse to

16 answer?

17 MR. PIOLI: Let's go back.

18 MR. ROACHE: Off the record.

19 THE VIDEOGRAPHER: Off the record at

20 2:45 p.m.

21 (Discussion off the record.)

22 THE VIDEOGRAPHER: On the record at

23 2:46 p.m.

24

Exhibit C

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

MINTEL INTERNATIONAL GROUP,)	
LTD., a United Kingdom corporation,)	
)	
)	
Plaintiff/Counter-Defendant,)	Case No. 08-cv-3939
)	Judge Robert Dow, Jr.
v.)	Magistrate Judge Maria Valdez
MEESHAM NEERGHEEN, an individual)	
)	
Defendant/Counter-Plaintiff.)	
_____)	

DECLARATION OF ANDREW REISMAN

I, Andrew Reisman, swear as follows:

1. I am over the age of eighteen, have personal knowledge of the facts described in this declaration, and if called as a witness would testify to the same.

2. As more fully set forth herein, I have reviewed the Affidavit of Scott R. Jones (the "Jones Affidavit") as well as the hard drive Mr. Jones identified as "Item 004," and in my opinion the Affidavit suffers from numerous defects that call into question virtually every conclusion reached therein. The Jones Affidavit reaches erroneous conclusions regarding alleged spoliation of evidence that in some instances are contradicted by the very facts the Affidavit cites, makes sweeping claims about matters beyond the scope of the available data, draws legal conclusions beyond the purview of a forensic examiner, and fails in any fashion to connect the activity cited to loss of any potentially relevant data. These inaccuracies, omissions

and overreaching, although presumably not a deliberate effort to mislead the Court, nevertheless culminate in conclusions that are divorced from the forensic evidence available for examination.

3. I am the President of Elijah Technologies, a company specializing in computer forensic investigations, electronic discovery and litigation support. I am based out of Elijah Technologies' Chicago headquarters, and my company also has offices nationally. Prior to founding Elijah Technologies in 2003, I was a partner practicing in litigation and technology law at Foley & Lardner in Chicago.

4. I am an expert in the fields of computer forensics and electronic discovery. As president of Elijah Technologies, I have supervised the harvesting and production of electronic discovery databases in well over 100 engagements, and routinely provide consulting services relating to electronic discovery production and data retention issues. I also have had primary responsibility for well over 100 computer forensic engagements involving well over 1000 computers and other forms of electronic media. I have earned certifications in the field including as an EnCase Certified Examiner (EnCE), and have been qualified as an expert in computer forensics and electronic discovery in Illinois, Florida and Michigan courts. I have served on the Board of Directors of the International Information Systems Forensics Association and have lectured on computer forensics at accredited CLE programs and as a guest speaker at Northwestern University, Illinois State University and the DePaul University School of Law. My CV is attached as Exhibit A.

The Jones Affidavit's Conclusions Regarding File Entry Activity After July 11, 2008 And Destruction Of Evidence Are Based On Legal Argument And Incomplete Forensic Evidence (Jones Aff. ¶¶ 7-11)

5. The Jones Affidavit posits that because Mr. Neergheen was served with notice of this litigation on July 11, 2008, he had a legal duty to immediately cease using the Item 004

computer because any activity thereon could change or overwrite data that theoretically could be relevant to the litigation. In fact, a significant portion of the Jones Affidavit is premised on a failure to adhere to that supposed legal duty.

6. The function of a computer forensic examiner is not to opine on what legal duties the parties to litigation have, but rather to examine and explain computerized data and describe how computers function in order to assist the finder of fact. Whether Mr. Neergheen legally was required to immediately cease using his computer is a determination more appropriately evaluated by the Court.

7. As pointed out in the Jones Affidavit, normal computer usage, even leaving a computer on without actively using it, potentially can result in the changing or overwriting of data on a computer. Although I express no opinion regarding what the legal standard for preservation is or should be, if all litigants were held to the legal standard the Jones Affidavit posits – that “the computer [should have been] turned off and left alone starting on July 11, 2008 ... following receipt of notice of active litigation” – many companies with regular litigation likely would find challenging meeting that requirement while still performing their normal business functions. I also am interested to learn whether Intel immediately ceased using all of its computers on which potentially relevant data resides.

8. Additionally, this and the other sections of the Jones Affidavit fail to make the critical distinction between data and evidence. It is undisputed that routine computer usage changes data, but whether such data is potentially relevant to particular litigation – i.e. constitutes evidence – requires a higher level of computer forensic analysis.

9. Here, the Jones Affidavit does not reference a single file or data artifact that he attempts to show evidences transmission of Intel trade secrets. Nor does the Jones Affidavit,

which points to updating of file Last Accessed dates as evidence spoliation, attempt to show that any of the updated files contains relevant evidence for which it would have been important to know when such files previously had been accessed. Rather, the only evidence that the Jones Affidavit presents directly relating to alleged Mintel trade secrets are Mr. Neergheen's own statements in that regard.

10. Accordingly, although certainly routine usage of Item 004 affected data contained on the drive, the assertion of the Jones Affidavit that such usage constitutes spoliation of evidence is unsupported by the forensic evidence presented therein.

11. The Jones Affidavit also points out that over 3900 file entries were created on or after July 13, 2008, but does not make any effort to describe the character of those files or their relative impact on the drive. This data was readily available for review by Mr. Jones, and in fact is incorporated into his "Item 004_AllFilesPresent" reports.

12. I have reviewed those files and found that nearly 3800 of them were associated with Internet browsing activity, such as temporary picture files and cookies. This is inconsistent with a deliberate attempt to overwrite the drive's unallocated space, and would have occurred without the user knowing those files were being written to the drive. Collectively the new data represented only approximately 223 megabytes of data, a small fraction of the amount of free space on the drive. Had Mr. Neergheen wanted to overwrite the unallocated space on the drive, he easily could have downloaded a few movies or other large files to the drive on or after July 11, 2008, but he did not do so. Rather, the available evidence is fully consistent with routine computer usage and not deliberate destruction of data.

The Jones Affidavit's Assertions Regarding Mr. Neergheen's Level of Computer Expertise Is Premised On Erroneous Assumptions (Jones Aff. ¶ 12)

13. Mr. Jones posits in his affidavit that he is “disinclined to accept at face value Mr. Neergheen’s deposition testimony that he is ‘...not a computer savvy person.’” (Jones Aff., ¶ 12) Mr. Jones bases this conclusion in part on the erroneous assumption that data not generally accessible to a novice computer user was deleted from Item 004 after July 11, 2008 at 6:00 p.m.

14. As discussed in more detail below, I have reviewed the files deleted after July 11, 2008 at 6:00 p.m., and the vast majority of those deleted files appear to be the result of Internet browsing activity. It takes little computer skill to delete such files, as that is an easily accessible option within Internet Explorer. Additionally, as also set forth in more detail below, for every one of the supposedly “deleted” registry entries the Jones Affidavit cites as evidence of Mr. Neergheen’s computer savvy, there is an active (i.e. not deleted) entry in the same location of the registry. The Jones Affidavit posits no explanation for why Mr. Neergheen would delete certain registry entries and leave identical active registry entries, and in fact did not even point out that such identical active registry entries were present.

The Evidence Is Inconsistent With The Jones Affidavit's Assertion That An Antivirus Scan Obscured Date And Time Metadata On Or After July 17, 2008 (Jones Aff. ¶¶ 13-15)

15. The Jones Affidavit asserts that on July 17 and July 18 there was file activity on Item 004 associated with McAfee antivirus software and asserted that “this further destroys evidence related to dates and times which would exist if not for the usage of antivirus software within Item 004.” (Jones Aff. ¶ 13) This statement suffers from one particularly significant

defect – the fact that there is no evidence in Item 004 that the McAfee virus scan caused mass updating of last access dates that changed pertinent metadata.

16. Mr. Jones observed that a file associated with McAfee antivirus software was executed on July 17, stated that running an antivirus program can update Last Accessed dates for files, and concluded that there was “Use of Antivirus Software to Obscure Date and Time Metadata” and that Mr. Neergheen “failed to stop automated system utilities from running that would destroy and/or alter evidence” (Jones Aff. ¶¶ 13, 15) Mr. Jones apparently did not examine the underlying file metadata or test the McAfee antivirus software before making that claim, however, because the McAfee virus scan software in fact did not and does not alter the file metadata of the files being scanned.

17. If Mr. Jones had analyzed the Last Accessed dates of files in Item 004, he would have seen that no mass updating of last access dates occurred on or after July 17, 2008. Of the nearly 95,000 files and folders in Item 004, less than 1200 were accessed on or after the activity the Jones Affidavit cites, and the majority of that activity related to new files created from Internet browsing activity rather than existing files having been newly accessed. This evidence is readily available from the “Item 004_AllFilesPresent” reports that Mr. Jones prepared and provided to the parties, and is inconsistent with his statement that the virus scan destroyed evidence by causing last access dates to update *en masse*.

18. Additionally, if Mr. Jones had tested the McAfee antivirus software on his own computer, he would have been able to confirm as I did upon testing that the McAfee antivirus software scan does not in fact update last access dates (or upon scanning immediately resets them to their previous state). The only files that would have their last access dates updated are

the few files associated with the McAfee program itself, such as the files identified in Table One of the Jones Affidavit, rather than substantive documents.

19. Moreover, even if a virus scan had been run and certain last access dates had been updated, the Jones Affidavit makes no effort to tie any such updated last access dates to documents containing alleged Mintel trade secrets. Apparently Mr. Jones could identify no potentially relevant files that were last accessed on or after July 17, 2008, as none are listed in his affidavit. Accordingly, there was no factual basis for the assertion in the Jones Affidavit that antivirus software was used to obscure date and time metadata and to destroy evidence.

The Jones Affidavit's Section Regarding "Spoliation Noted Within Item 004 Internet History" Does Not Establish Spoliation Of Evidence (Jones Aff. ¶¶ 16-24)

20. The section of the Jones Affidavit entitled "Spoliation Noted Within Item 004 Internet History" establishes what Mr. Neergheen already has admitted – that he ran a search in Microsoft's online support site for "how do i access deleted" files. (Jones Aff. ¶ 20) Mr. Jones testified that in preparing his Affidavit he performed the same search on his computer, found a number of different help articles, and concluded that Mr. Neergheen must have read one of the help files regarding how to delete certain information and subsequently made such deletions.

21. This leap in logic is not supported by the available forensic evidence. If just one day before Item 004 was forensically imaged Mr. Neergheen had accessed help files detailing how to delete registry data, evidence of viewing such help files likely would be present on the drive. The Jones Affidavit presents no such forensic evidence. Instead, the Jones Affidavit ignores the nature of the search – how to access deleted files, not how to delete files – and cherry picks from the associated hits in the Microsoft Knowledge Base the article title that most

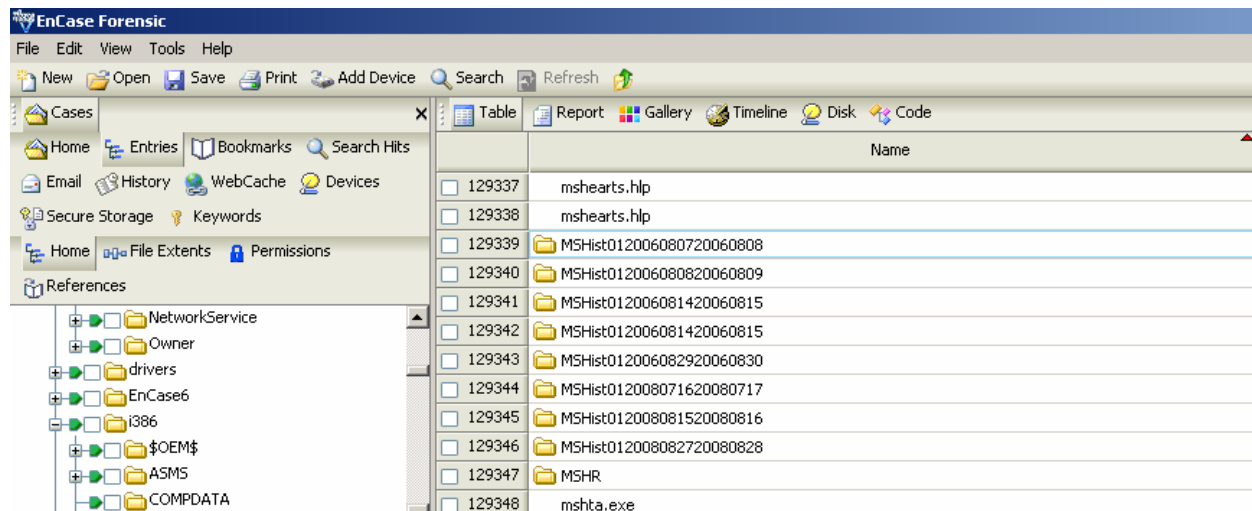
supports his client's motion and posits that Mr. Neergheen reviewed that article. That is advocacy, not forensic analysis.

The Jones Affidavit's Allegations Regarding Missing Internet History Data Are Erroneous (Jones Aff. ¶¶ 25-28)

22. The Jones Affidavit contends that Mr. Neergheen must have deleted Internet history because there are gaps in the MSHist daily and weekly entries. Those allegations are based on a fundamental misunderstanding of how the MSHist file entries function.

23. The Jones Affidavit leaves the incorrect impression that an MSHist file entry is created for every day that a person uses the Internet. That simply is incorrect. Rather, MSHist entries are created based on the settings in Internet Explorer for the number of days the user wishes to store Internet history. If the number is set to 20 (the maximum number), there would be 20 MSHist entries. If the number is set to zero, there would be none. Here, there were 11 MSHist entries associated with Mr. Neergheen's user profile. The fact that there was not an MSHist entry for every day during which Mr. Neergheen used the Internet is normal, rather than evidence of deletion activity.

24. To test this, I used EnCase to preview the MSHist entries on my own computer. I have used my computer on a regular basis during the course of the past year, and routinely access the Internet. The following is a screenshot showing all MSHist entries on my computer:



25. This screenshot shows a total of eight MSHist entries on my computer. Five of those entries are from August 2006, one is from July 2007, and two are from August 2008. According to the logic of the Jones Affidavit, these pronounced gaps are the result of a clever attempt to destroy Internet history. I have never taken any steps to delete MSHist files on my computer, have used the Internet regularly on the computer, and the “gaps” are still present. This is further proof that the gaps are an artifact of how the software operates, not the product of a sophisticated attempt by Mr. Neergheen to delete Internet history.

26. Moreover, even if Mr. Neergheen had deleted all MSHist entries (which he did not), those entries do not contain detailed artifacts of which web sites have been visited and when and accordingly are not the best source for analyzing Internet activity. Rather, the index.dat files contain such data, and my analysis of those files reveals fairly consistent use of the Internet during the period of time during which Mr. Jones claims gaps exist. In fact, Mr. Jones prepared Internet History reports which he provided to both parties, which reports detail thousands of entries showing dates, times, and web addresses of sites visited on Item 004 during the period of time during which the Jones Affidavit claims gaps exist. Mr. Jones’ claim that “[t]he daily information appears to have been selectively deleted while the weekly information

prior to June 23, 2008 was deleted *en masse*” has absolutely no basis in forensic evidence, and ignores the very evidence presented in his own reports to the contrary.

The Jones Affidavit’s Assertions Regarding Spoliation Within The Registry Reported By The USBSTOR Report Are Inaccurate, As Active Registry Data Is Present For All Listed USB Devices (Jones Aff. ¶¶ 29-39)

27. The Jones Affidavit asserts that Mr. Neergheen targeted a specific portion of the Windows registry for deletion that contained data regarding which USB devices had been inserted into Item 004, but this simply is inaccurate. For every one of the USB entries listed in Table Five of the Jones Affidavit as “deleted” there also exists a corresponding entry with the same date, time and device that is an active, non-deleted entry.

28. As proof of that, I reviewed the Item004_USBSTOR report Mr. Jones created, and confirmed that ID#1 is an identical active registry entry corresponding to ID#2 in Table Five, ID#15 is active and corresponds to ID#11, ID#22 is active and corresponds to ID#21, ID#30 is active and corresponds to ID#29, and ID#65 is active and corresponds to ID#63.

29. Accordingly, all of the supposedly “deleted” registry entries have equivalent identical active entries in the registry. The assertion of the Jones Affidavit that this data was spoiled in some fashion is patently erroneous, and other conclusions that Mr. Jones draws from this alleged deletion activity, such as Mr. Neergheen’s level of computer savvy, are also called into question.

30. Moreover, even if identical active entries did not exist, the Jones Affidavit establishes that there was no spoliation of evidence. All of the registry entries to which Mr. Jones cites were fully viewable using his forensic software, and he was able to identify the

specific USB devices in question and dates of insertion. Mr. Jones does not explain how the registry data was spoiled given that he could fully view and analyze it.

The Fact That Link Files Show Access Of Certain Data Adds Nothing Meaningful For Review By The Finder Of Fact (Jones Aff. ¶¶ 40-43)

31. The Jones Affidavit cites to link files as evidence that Mr. Neergheen used USB storage devices and accessed files on the Internet, which Mr. Neergheen freely has admitted. Nothing in the Jones Affidavit, however, establishes that the link files relate to alleged Mintel trade secrets.

32. The link files the Jones Affidavit cites provide the names of the files accessed. If Mintel recognized those names as containing its trade secrets, presumably it would have brought that to the Court's attention. I am not aware of Mintel having done so, and it was not done in the Jones Affidavit.

The Jones Affidavit Erroneously Claims That There Was Spoliation Within The Item 004 Windows Prefetch File Entries (Jones Aff. ¶¶ 44-51)

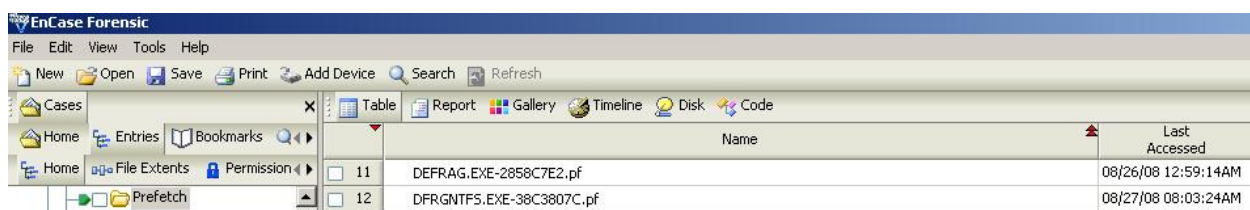
33. The Jones Affidavit asserts that on July 14, 2008 the Item 004 hard drive was defragmented using the Windows defragmentation utility, and that he "found no indication that defrag was run as part of an automated system process, which suggests that someone ran this utility deliberately on July 14, 2008." (Jones Aff. ¶ 48) To the contrary, however, the evidence is clear that defrag was run on that date as an automated system process rather than the deliberate act of Mr. Neergheen, and the very proof of that fact is contained in the Table 7 of the Jones Affidavit two pages later.

34. On a computer running Windows XP and formatted with the NTFS file system, as was Item 004, two files are primarily associated with file defragmentation: dfrgntfs.exe and

defrag.exe. By default, when Windows XP enters an idle state for a pre-set period of time it will launch the dfrgntfs.exe and defrag.exe files, which begins the automated process of defragmenting the hard drive in order to improve system performance. When this process is done on an automated basis by the Windows XP operating system, the associated files in the Prefetch directory would have identical Last Written dates and times.

35. When defragmentation is initiated by a user, as opposed to the automated process initiated by Windows XP, the file in the Prefetch directory associated with dfrgntfs.exe would have a later Last Written date than the file in that directory associated with defrag.exe. That is because a user directed defragmentation is initiated through the dfrgntfs.exe file alone and does not update the Prefetch file associated with defrag.exe, whereas the automated defragmentation process accesses both files and updates both associated entries in the Prefetch directory.

36. To test and demonstrate this, on the morning of August 27, 2008 I initiated a defrag process on my home computer. Using forensic software I then examined the dates and times of the defrag.exe and dfrgntfs.exe entries in the Prefetch directory and confirmed that the dfrgntfs.exe entry was more recent than the defrag.exe entry as shown below:



	Name	Last Accessed
11	DEFRAG.EXE-2858C7E2.pf	08/26/08 12:59:14AM
12	DFRGNTFS.EXE-38C3807C.pf	08/27/08 08:03:24AM

37. This screenshot confirms that a deliberate, user initiated defragmentation would result in the dfrgntfs.exe file in the Prefetch directory having a later last access than the associated defrag.exe file, whereas in the case of Item 004, the time entries were the same, proving that the defragmentation was the result of an automated system process. I can also confirm that it was months before that I previously deliberately had initiated a defrag process on

my personal computer, whereas the last access date for the defrag.exe file in the Prefetch directory showed that defrag had been run on 8/26/2008 at 12:59 a.m. – further demonstrating that Windows XP by default initiates defragmentation processes when the system is idle for a pre-set period of time.

38. Here, the evidence in Item 004, and set forth in Table 7 of the Jones Affidavit, clearly shows that both files in the Prefetch directory (here DEFRAG.EXE-273F131E.pf and DFRGNTFS.EXE-269967DF.pf) have identical dates and times, July 14, 2008 at 6:39:05 p.m. This establishes that the file defragmentation of that date was the result of an automated process common to the millions of computers configured similarly to Item 004, and does not evidence a deliberate attempt by Mr. Neergheen to defragment his hard drive as suggested by the Jones Affidavit.

39. The functions of the defrag.exe and dfrgntfs.exe files and their associated Prefetch directory entries, and how to interpret them in determining whether defragmentation was deliberate versus an automated system function, are well known to experienced computer forensic investigators and the analysis I have performed in that regard is widely accepted in the field as a method for making such a determination.

40. In addition to his opinions relating to defragmentation, Mr. Jones opines that “other prefetch file entries report creation and/or being last written on July 17, 2008 ... [which] necessarily overwrites previously unallocated space which contained evidence.” (Jones Aff. ¶ 49) This statement is inaccurate on multiple levels.

41. *First*, updating of existing prefetch file entries would merely change dates associated with those file entries, and would have absolutely no effect on the unallocated space of the drive. Every one of the prefetch file entries in Table Seven of the Jones Affidavit

constituted updating of an existing entry, and would have had no impact on the drive's unallocated space.

42. *Second*, I reviewed the Item004_AllFilesPresent report Mr. Jones prepared, and confirmed that only three new prefetch entries were created on or after July 11, 2008, comprising only 51 kilobytes of data. The creation of those 51 new kilobytes of data – the size of a small word processing document – had a negligible impact relative to the amount of data in the unallocated space. It would have taken approximately 150,000 such new file entries to overwrite the Item 004 unallocated space, not the three entries that actually were new. Again, this information was readily available in the reports Mr. Jones prepared for the parties.

43. *Third*, it is a substantial leap in logic that the tiny amount of data written to the drive actually overwrote evidence. A forensic examiner could attempt to prove evidence was lost by looking at the slack space of those files – residue from data previously occupying the same drive space – and showing that it contained a fragment of relevant evidence of which the new file overwrote surrounding data. Mr. Jones did not present such evidence, presumably because there was no evidence that the new files overwrote a portion of any relevant evidence.

The Jones Affidavit's Conclusions Are Based On Flawed Premises And Are Accordingly Unreliable (Jones Aff. ¶¶ 52-58)

44. The Jones Affidavit draws numerous conclusions about Mr. Neergheen's intentions, but those conclusions are based on the erroneous premises Mr. Jones reached as demonstrated above. Moreover, Mr. Jones' supposition that Mr. Neergheen intended to hide data, copied the data to USB devices that Mr. Jones has not yet examined, moved the data to other locations that he also has not yet examined, and that the data he has not examined actually

contained Mintel trade secrets (Jones Aff. ¶¶ 39, 53-54), collectively are well beyond the range of what Mr. Jones has data to support. These conclusions are advocacy, not forensic analysis.

45. In my opinion the forensic evidence presented in the Jones Affidavit does not support his conclusions that Mr. Neergheen deliberately destroyed data or that any relevant evidence was lost.

I declare, pursuant to 28 U.S.C. 1746 and under penalty of perjury that the foregoing is true and correct.

Executed on August 29, 2008

A handwritten signature in black ink, appearing to read 'Andrew Reisman', is written over a horizontal line.

Andrew Reisman

Andrew Reisman

Elijah Technologies, Ltd.
866-354-5240 x101
andy@elijahtechnologies.com
www.elijahtechnologies.com

Professional History

Current Employment
➤ President, Elijah Technologies
➤ President, LITIGEX

Previous Employment
➤ Partner, Enterprise Law Group
➤ Partner, Foley & Lardner
➤ General Counsel, International Save the Children Alliance
➤ Associate, Mayer, Brown & Platt
➤ Judicial Clerk, Hon. Harlington Wood, Jr., U.S. Court of Appeals

Educational History

University of Illinois College of Law, J.D. *Summa Cum Laude*
➤ Class Valedictorian
➤ Editor-in-Chief, Law Review
➤ Order of the Coif

Illinois State University, B.S., *Magna Cum Laude*
➤ University Honors Scholar
➤ President, Forensics Union

Training & Associations

➤ EnCase Certified Examiner (EnCE)
➤ Certified Fraud Examiner (CFE)
➤ Electronic Evidence Specialist (BES)
➤ Executive Committee & Board of Directors, International Information Systems Forensics Association (IISFA)
➤ Past President, Chicago Chapter, IISFA
➤ Board of Directors, Illinois State University Attorneys Advisory Board
➤ Member, GLG Councils
➤ Marquis' Who's Who in America, 2006
➤ Certificate, EnCase Advanced Computer Forensics

Publications & Speeches

➤ *Electronic Evidence And Computer Forensics: A Brief Primer*, IICLE Law Office Technology Flash Points
➤ Guest Lecturer on Topics in Computer Forensics & E-Discovery, Chicago Bar Association, DePaul University, Northwestern University, Illinois State University and various firms and corporations
➤ CBA Commercial Litigation Mock Trial Expert Witness, Computer Forensics, 2007

Andrew Reisman, EnCE CFE JD

Andrew Reisman is President of Elijah Technologies, a legal technology company specializing in computer forensic investigations, e-discovery, and litigation support. Andrew has had primary responsibility for hundreds of investigations and has testified and lectured on numerous occasions regarding computer forensics and electronic discovery. As a litigation consultant, Andrew frequently is called upon to manage sophisticated document intensive projects on a turnkey basis, harvest or oversee the harvesting of electronic data, provide advice regarding e-discovery best practices, and manage vendor qualification and bidding. Drawing upon his extensive computing, forensic investigation, and legal backgrounds, Andrew is uniquely qualified to bridge the communication gaps that so frequently arise between inside and outside counsel, IT/IS departments, and finders of fact, and to most efficiently and expeditiously identify key case evidence.

Computer Forensic Experience

- Led investigations for Fortune 500 institutions and a variety of corporate and law firm clients. Engagements included devising investigation parameters, imaging hundreds of drives and other electronic media, identifying potential sources of evidence, reviewing collected data for responsive and deleted files, preparing reports, and testifying regarding findings.
- Recent Testimony: *Smith v. Effective Teleservices, Inc.*, 15th Judicial Circuit, Palm Beach County, Florida (2008) – In a matter on behalf of a telecommunications company, provided testimony regarding alleged spoliation of computerized evidence and analysis of report prepared by opposing computer forensics expert.
- Recent Testimony: *Dematic Corp. v. Tubman*, Kent County Circuit Court, Grand Rapids, Michigan (2008) – In a matter on behalf of an automation company, identified electronic evidence of trade secret misappropriation and provided related testimony on which the Court relied in enjoining the former employee from competing against the employer.
- Recent Testimony: *AD Acquisition, LLC v. Lyon*, Circuit Court of Cook County, Chicago, Illinois (2007) – In a matter on behalf of an auto transport company in a trade secret misappropriation dispute, provided testimony regarding spoliation of computerized evidence on which the Court relied in entering a default judgment in favor of client.
- Recent Testimony: *MEPCO, L.L.C. v. MC Squared of Michigan, L.L.C.*, Kent County Circuit Court, Grand Rapids, Michigan (2007) – In a matter on behalf of a manufacturing company, investigated computer media for evidence of breach of fiduciary duty. Located evidence of deleted emails and testified at preliminary injunction hearing regarding findings.
- Recent Testimony: *Peter Gombrich v. Molecular Diagnostics, Inc.*, ADR Systems of America, Chicago, Illinois (2006) – In a matter on behalf of a technology company, investigated computer media for destruction of data. After locating evidence of same and testifying at arbitration hearing, client secured favorable spoliation finding.

Litigation Consulting Experience

- Provided consulting services relating to large document review projects, including overseeing data harvesting, vendor qualification, proposal drafting and evaluation, database consulting and overall project management.
- Designed and implemented data filtering and collection programs to efficiently search and collect terabytes of data for export to e-discovery platforms.
- Case Highlight: Turnkey Consulting – In a matter on behalf of a large consumer product company provided client with advice regarding restoration of thirty terabytes of data, document retention and litigation hold policies, and data hosting platforms.

E-Discovery Experience

- Leads the Elijah Technologies team recognized by the 2006 Socha-Gelbmann Electronic Discovery Survey as a top-20 provider nationally in e-discovery capacity.
- Oversees filtering, processing and hosting of multi-terabyte collections of data.

EXHIBIT D

Intentionally Omitted

EXHIBIT E

Clark, Geraldine

From: Lervick, Jeana R. [jlervick@bellboyd.com]
Sent: Thursday, September 04, 2008 3:30 PM
To: Clark, Geraldine
Subject: FW: Mintel v. Neergheen; Case No. 08CV3939; Temporary Restraining Order

-----Original Message-----

From: Katherine J. Pronk [mailto:pronkk@jbltd.com]
Sent: Tuesday, July 15, 2008 9:07 AM
To: Proposed_Order_Dow@ilnd.uscourts.gov
Cc: Joseph Marconi; Lervick, Jeana R.
Subject: Mintel v. Neergheen; Case No. 08CV3939; Temporary Restraining Order

Judge Dow:

Please find attached Plaintiff's Proposed Order for the emergency hearing on Plaintiff's requested Temporary Restraining Order scheduled for today at 10:00 a.m. This correspondence is also being sent to Defendant's counsel, Jeana Lervick of Bell, Boyd and Lloyd, LLP.

Please advise if you have any problems opening or viewing the Proposed Order. Thank you.

Katherine J. Pronk
Johnson & Bell, Ltd
33 W. Monroe St.
Suite 2700
Chicago, IL 60603
dir 312.984.0287
fax 312.372.9818
www.johnsonandbell.com

All contents of this e-mail and any attachment are private & confidential. If received or viewed by anyone other than the intended recipient, neither this e-mail nor any attachments, or anything derived from these, may be used or passed on for any purpose whatsoever, and all materials must be destroyed and the sender notified immediately.

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

MINTEL INTERNATIONAL GROUP,
LTD., a United Kingdom corporation,

)

Case No.: 08CV3939

)

Judge Robert Dow, Jr.

)

)

)

)

ORDER

This cause coming to be heard upon Plaintiff MINTEL INTERNATIONAL GROUP's Motion for Temporary Restraining Order, Joseph R. Marconi and Victor J. Pioli of Johnson & Bell, Ltd. appearing for Plaintiff, and Bell, Boyd & Lloyd, LLP appearing for Defendant MEESHAM NEERGHEEN, and the Court being fully advised in the premises, IT IS HEREBY ORDERED:

1. Based upon the pleadings filed by Plaintiff and the argument of counsel in open court, the Court finds that Plaintiff has sustained its burden and demonstrated a likelihood of success on the merits of its claims. The Court also finds that Plaintiff does not possess an adequate remedy at law and will suffer irreparable harm should a temporary restraining order not be issued. The balance of harms and public interest are also served by the issuance of a temporary restraining order.

2. Pursuant to Federal Rule of Civil Procedure 65, a ten (10) day temporary restraining order, commencing at 10:00 a.m. on July 15, 2008 and expiring at 10:00 a.m. on July 29, 2008, is entered upon the following terms and conditions:

A. Defendant, his agents, servants, employees, officers, attorneys, successors and assigns, and all persons, firms, and corporations acting in connection or participation with him or on his behalf, are enjoined from using, referencing, evaluating, or copying all originals and copies of information or documents misappropriated from Mintel in hard copy or electronically stored;

B. Defendant, his agents, servants, employees, officers, attorneys, successors and assigns, and all persons, firms, and corporations acting in connection or participation with him or on his behalf, are enjoined from revealing or disclosing in any manner information and documents misappropriated from Mintel in hard copy or electronically stored;

C. Defendant is required to return to Mintel all copied, printed, and/or downloaded files, materials, and information taken from Mintel;

D. Defendant is required to produce forensic copies of all personal desktop and/or laptop computers;

E. Defendant, his agents, servants, employees, officers, attorneys, successors and assigns, and all persons, firms, and corporations acting in connection or participation with him or on his behalf, are prohibited from deleting any files from Defendant's personal desktop and/or laptop computer related to or taken from Mintel;

F. Defendant is prohibited from contacting or soliciting any Mintel customer or client that Defendant had contact with during the last twelve (12) months of his respective employments with Mintel;

G. Defendant is prohibited from working for Datamonitor or any other competitor of Mintel; and

H. Defendant is prohibited from soliciting or contacting any Mintel employee for purposes of working at Datamonitor or any other competitor of Mintel.

3. Plaintiff's request for expedited discovery is granted. The parties may commence discovery at once. Written discovery responses are due within seven (7) days of service. Defendant shall appear for his deposition within ten (10) days.

4. This matter is set for status on Tuesday, July 29, 2008 at ____ a.m. in Room 1919.

JUDGE: _____

JUDGE'S NO.: _____

Date: July 15, 2008

EXHIBIT F

Carr, Richard 8/27/2008 9:26:00 AM

1 IN THE UNITED STATES DISTRICT COURT
2 FOR THE NORTHERN DISTRICT OF ILLINOIS
3 EASTERN DIVISION

4
5 MINTEL INTERNATIONAL GROUP,)
6 LTD., a United Kingdom)
7 Corporation,)
8 Plaintiff,)
9 vs.) No. 08 CV 3939

10 MEESHAM NEERGHEEN, an)
11 individual,)
12 Defendant.)

13
14 Videotaped Deposition of RICHARD CARR,
15 taken before GREG S. WEILAND, CSR, pursuant to the
16 Federal Rules of Civil Procedure for the United
17 States District Court pertaining to the taking of
18 depositions, at Suite 2800, 70 West Madison Street,
19 in the City of Chicago, Cook County, Illinois,
20 commencing at 9:26 o'clock a.m., on the 27th day of
21 August, 2008.

22
23
24

1 so ...

2 Q. Did anyone instruct you not to delete any

3 e-mails relating to this litigation?

4 A. No.

5 Q. Have you made a forensic copy of your hard

6 drive?

7 A. No.

8 Q. Do you use a laptop or --

9 A. No, I use a --

10 Q. -- desktop?

11 A. -- desktop.

12 Q. Have you continued to use that since this

13 litigation began?

14 A. Yes.

15 Q. Have you printed out copies of any e-mails

16 you have relating to this litigation?

17 A. I don't know. I might have done the odd

18 one, but don't normally do, so ...

19 Q. Did you have any e-mail communications

20 with Mr. Weeks regarding this litigation?

21 A. There might be.

22 Q. Did you have any e-mail communications

23 with Mr. Butcher regarding this litigation?

24 A. Possibly. Probably.

CERTIFICATE OF SERVICE

The undersigned counsel hereby certifies that a true and correct copy of Neergheen's **Motion for Leave to File**, and accompanying documents including his Opposition to Mintel's Motion for Rule to Show Cause Regarding Temporary Restraining Order and Cross-Motion to Exclude Plaintiff's expert's Affidavit, have been served 4th day of September, 2008 via ECF filing to:

Joseph Marconi
Victor Pioli
Katherine J. Pronk
JOHNSON & BELL, LTD.
33 West Monroe Street
Suite 2700
Chicago, Illinois 60603

/s/ Jeana R. Lervick

Jeana R. Lervick
BELL, BOYD & LLOYD LLP
70 West Madison Street
Suite 3100
Chicago, IL 60602
(312) 373-1121